

The background of the slide is a photograph of a person's hand holding a small, white, hexagonal object with a keyhole in the center. The hand is wearing a light blue denim sleeve. The background is a solid light green color.

# FortiOS 6.2 – Whats New

FortiManager 6.2

Martin Ruesch – Security Consultant ALSO Schweiz

---

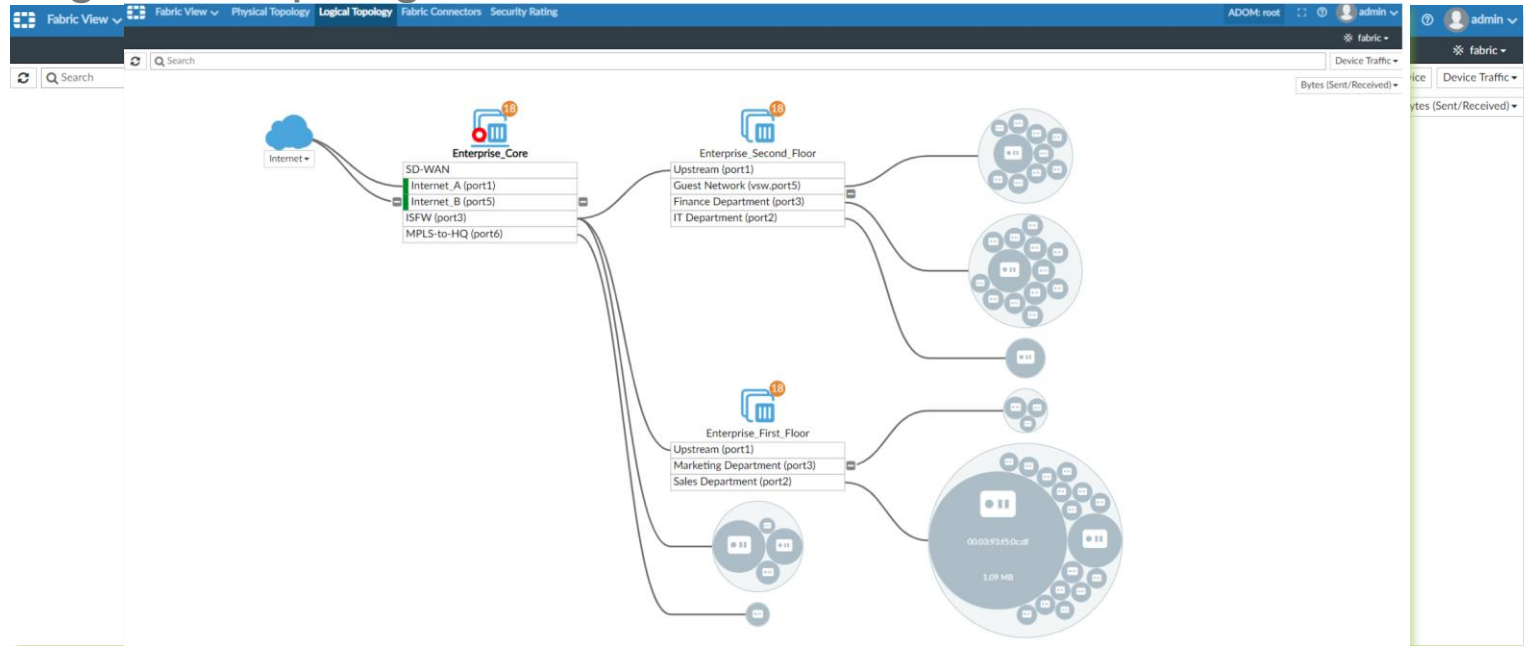
# Agenda

- ▶ Expanding Fabric
- ▶ SD-WAN
- ▶ Multi-Cloud
- ▶ Usability
- ▶ Compliance
- ▶ Other

# Expanding Fabric

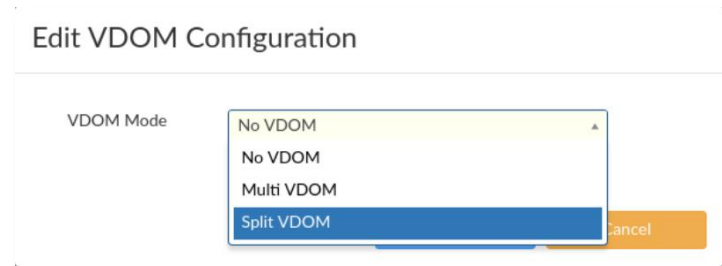
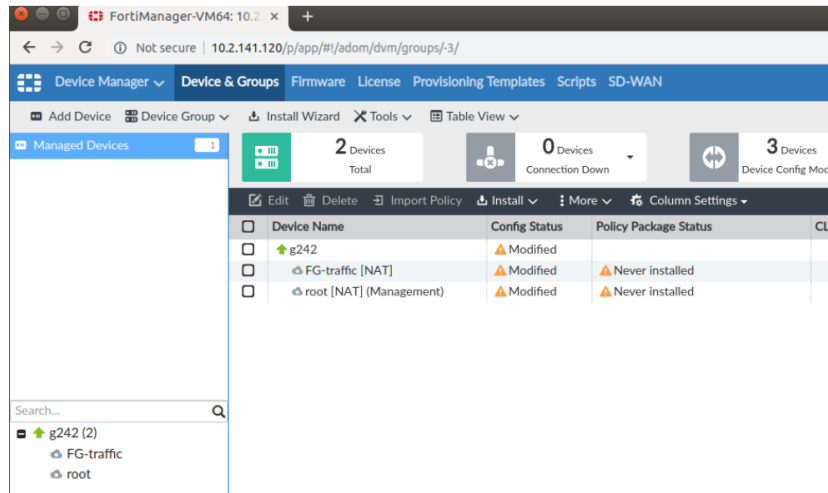
# Security Fabric Deployments – Physische Topologie

- ▶ Physische Topologie
- ▶ Logische Topologie



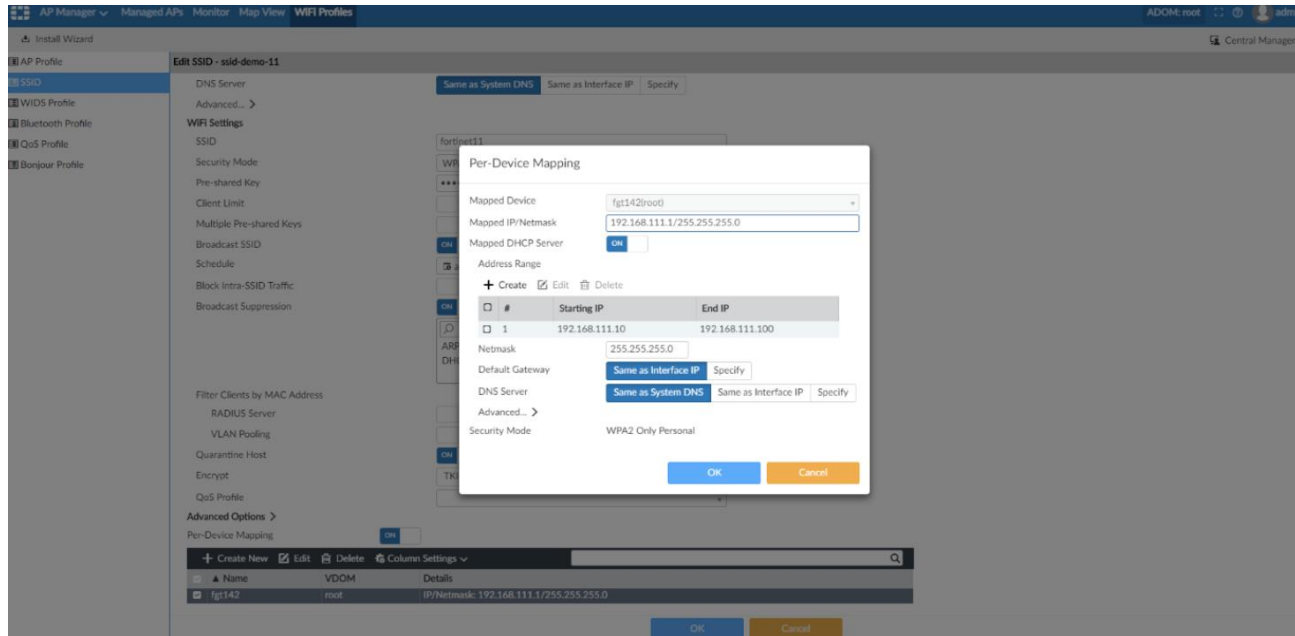
# Split Task VDOM Mode Support

- ▶ *No VDOM* es können keine VDOMs erstellt werden.
- ▶ *Multi VDOM* so viele VDOM wie die Lizenz hergibt können erstellt werden
- ▶ *Split VDOM* speziell mit 2 VDOM (1 Regulär, 1 Management)



# Dynamic Mapping für SSID

- Dynamisch Netze einer SSID per FortiGate zuweisen (gleiche SSID verschiedene Netze)



# SD-WAN

# IPSEC Wizard in Device Manager

- ▶ System Settings → All ADOMS editieren der ADOM. Deaktivieren der SD-WAN Option im Central Management
- ▶ Device Manager → SD-WAN jetzt Device oder ADOM auswählen.
- ▶ Jetzt Create VPN unter den Interface Members auswählen.

Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts **SD-WAN** ADOM: fgt62 admin ▾

Install Wizard Per-device Management

**SD-WAN** Edit SD-WAN

Monitor

Device FGVM020000155864 (root)

SD-WAN Status ☒ ON

Interface Members

+ Create New Edit Delete Move Up Move Down

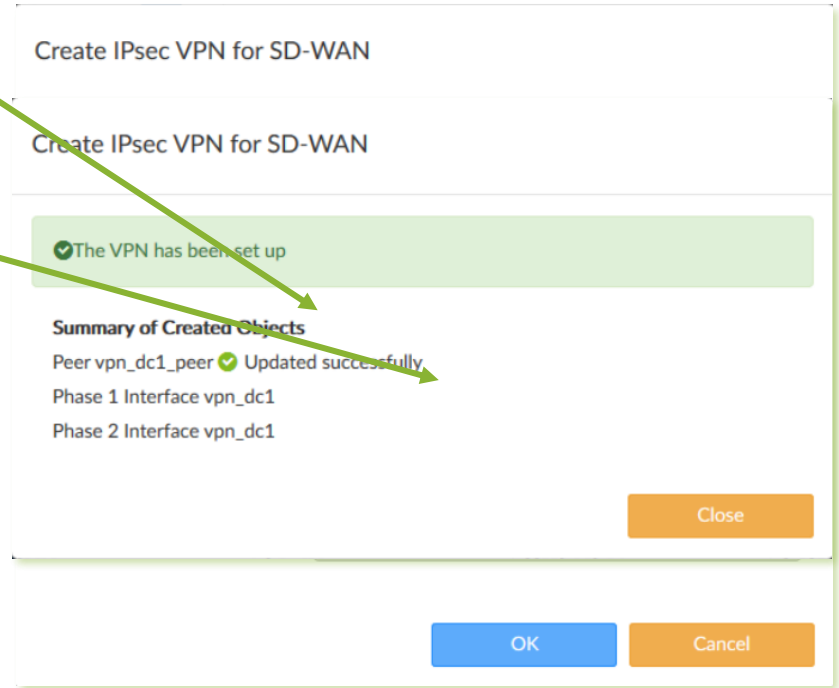
<input type="checkbox"/>	#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
<input type="checkbox"/>	1	4	port2	Enable	0	11.1.1.200	0	0
<input type="checkbox"/>	2	5	port3	Enable	0	12.1.1.200	0	0

Create VPN



# IPSEC Wizard in Device Manager

- ▶ Die ausgehenden Interfaces konfigurieren
- ▶ Authentication Methode: Pre-shared Key oder Zertifikat auswählen.
- ▶ Mit OK bestätigen, dann wird der Tunnel automatisch generiert.



# IPSEC Wizard in Device Manager

- ▶ Das automatisch erstellte VPN-Interface wird in der SD-WAN Interface Member Liste jetzt aufgeführt.
- ▶ Dem VPN Interface die Gateway IP und Up/Downstream konfigurieren.
- ▶ Der Konfigurierte VPN Tunnel ist

SD-WAN Status ☒ ON

**Interface Members**

+ Create New ☒ Edit ☐ Delete ☐ Move Up ☐ Move Down

<input type="checkbox"/>	#	ID	Port	Status	Weight
<input type="checkbox"/>	1	4	port2	✓ Enable	0
<input type="checkbox"/>	2	5	port3	✓ Enable	0
<input type="checkbox"/>	3	1	vpn_dc1	✓ Enable	

Create VPN

**Edit Member**

Member

Gateway IP

Status ☒ ON

Estimated Upstream Bandwidth (Kbps)

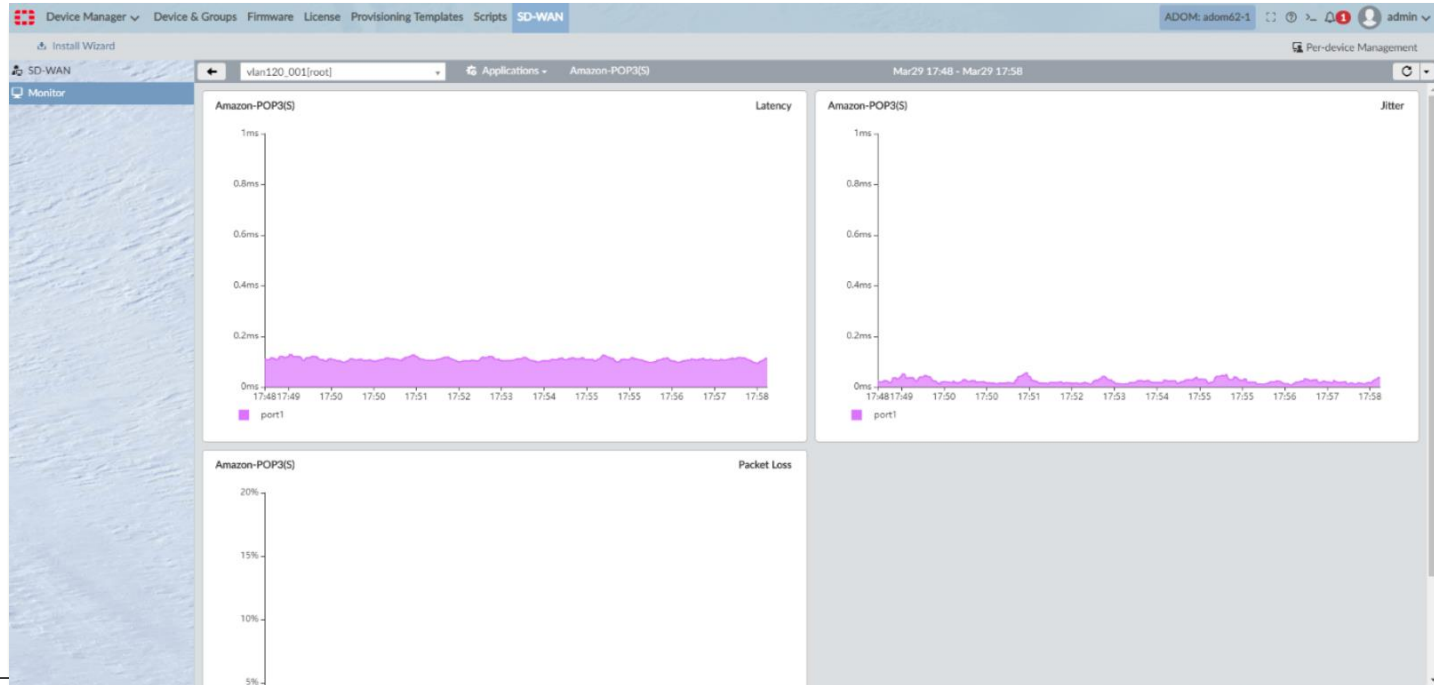
Estimated Downstream Bandwidth (Kbps)

**Advanced Options >**

OK Cancel

# SD-WAN History Monitoring

## ► Device Interface, Packet Loss, Bandwidth, Delay, Jitter History



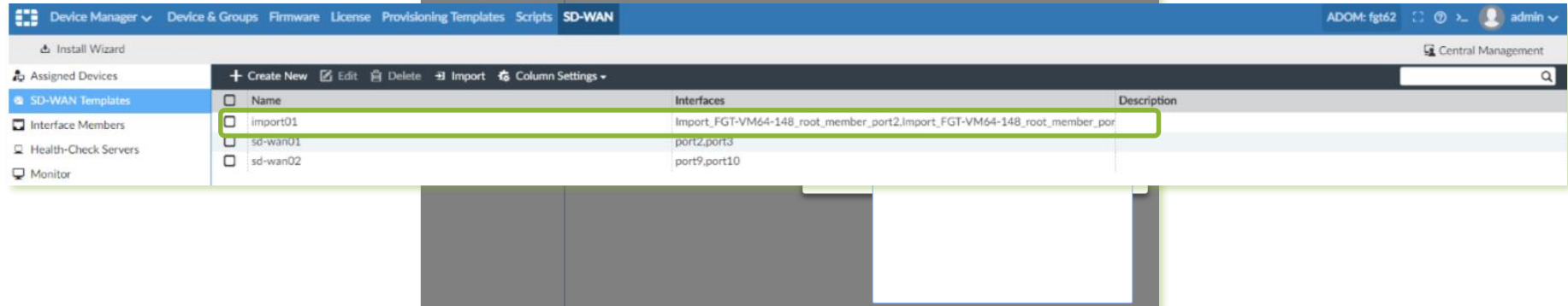
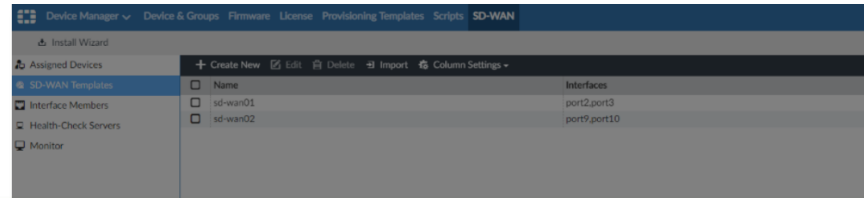
# SD-WAN History Monitoring

- ▶ Die Funktion muss auf der CLI aktiviert werden.
- ▶ Default mässig ist die Funktion disabled
- ▶ Wenn die Funktion disabled ist, werden nur die letzten zehn Minuten angezeigt.

```
config system admin setting
    set sdwan-monitor-history [enable|disable]
end
```

# SD-WAN Templates vom Device importieren

- ▶ Device Manager → SD-WAN → SD-WAN Templates
- ▶ Nach dem import wird das Template angezeigt.



# SD-WAN Templates vom Device importieren

- Die Interface Members, Performance SLA und SD-WAN-Regeln werden ebenfalls importiert.

The screenshot shows the FortiManager interface with the 'SD-WAN' tab selected. The 'Edit import01' dialog is open, displaying the configuration for an imported SD-WAN template. The left sidebar shows the navigation menu with 'SD-WAN Templates' selected. The main area is divided into three sections: 'Interface Members', 'Performance SLA', and 'SD-WAN Rules'.

**Interface Members**

#	ID	Port
1	1	Import_FGT-VM64-148_root_member_port2
2	2	Import_FGT-VM64-148_root_member_port3

**Performance SLA**

#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
1	lp_ts2	Import_FGT-VM64-148_root_health_lp_ts2	PING	5	5
2	ping2	Import_FGT-VM64-148_root_health_ping2	PING	5	5
3	ping3	Import_FGT-VM64-148_root_health_ping3	PING	5	5
4	ping_corp_gw	Import_FGT-VM64-148_root_health_ping_corp...	PING	5	5

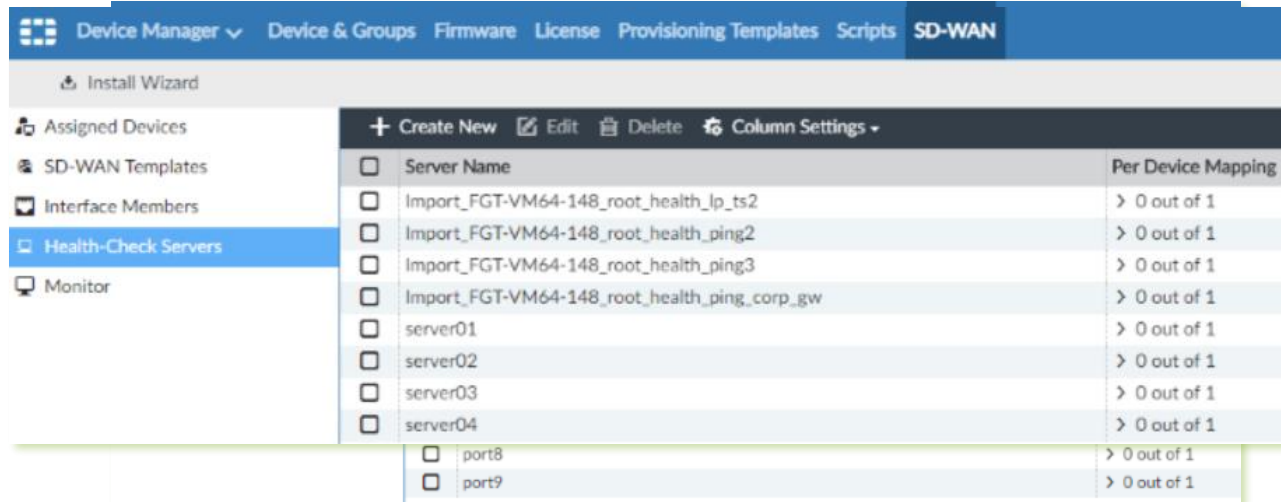
**SD-WAN Rules**

#	Name	Source	Destination	Criteria	Members
1	rule01-auto	ALL	all	Latency (lp_ts2)	ALL
2	rule02-manual	ALL	all	Latency	Import_FGT-VM64-148_root_member_port3
3	rule03-priority	ALL	Microsoft-Skype	Latency (ping3)	Import_FGT-VM64-148_root_member_port2
4	rule04-sla	ALL	Microsoft-Skype	ping2#1	Import_FGT-VM64-148_root_member_port2
5	rule05-load-balance	ALL	Microsoft-Skype	ping_corp_gw#1	Import_FGT-VM64-148_root_member_port2

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

# SD-WAN Templates vom Device importieren

- ▶ Nach dem import wird ein Name für jedes Mitglied generiert:  
`Import_{device-name}_vdom-name}_member_{interface-name}`
- ▶ Dasselbe wird auch mit den Healthcheck Server generiert:  
`Import_{device-name}_{vdom-name}_health_{health-check-name}`

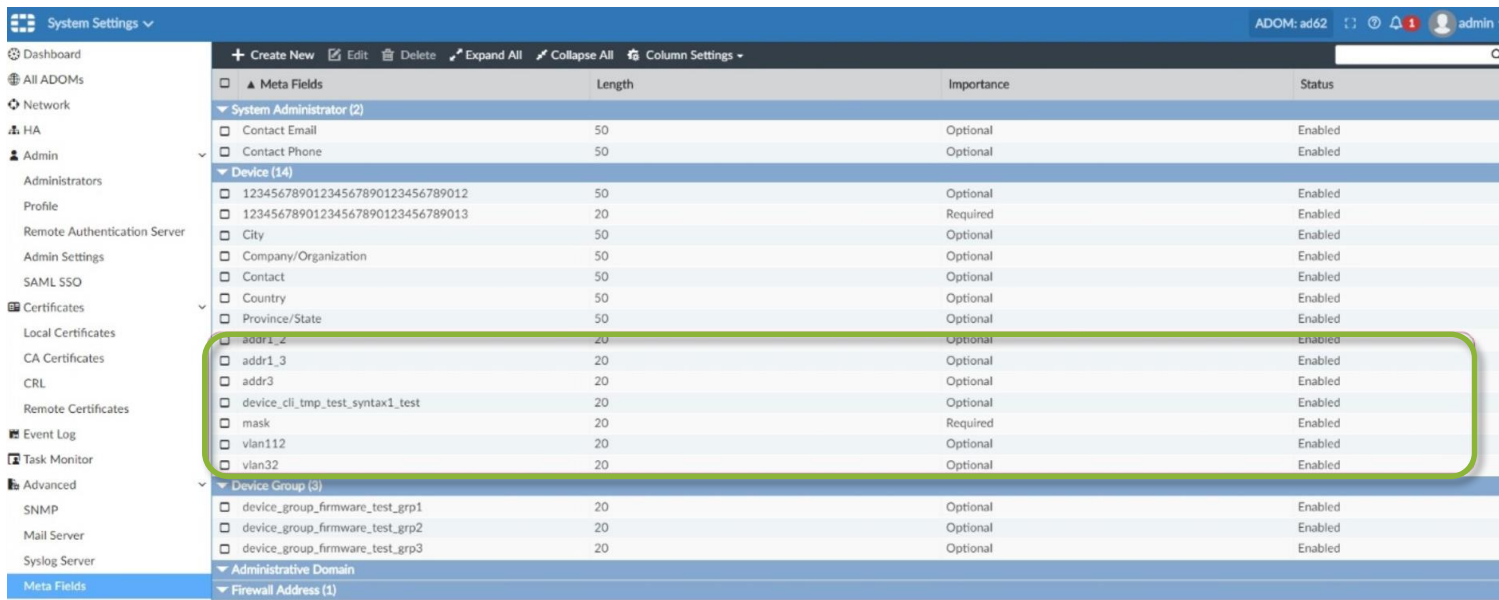


The screenshot shows the FortiManager web interface with the 'SD-WAN' tab selected. The left sidebar contains a tree view with 'Health-Check Servers' highlighted. The main panel displays a table of health-check servers with columns for 'Server Name' and 'Per Device Mapping'. The table lists several servers, including those generated by the import process (e.g., 'Import\_FGT-VM64-148\_root\_health\_ping2') and standard servers (e.g., 'server01' through 'server04'). Each server has a checkbox in the 'Per Device Mapping' column.

Server Name	Per Device Mapping
<input type="checkbox"/> Import_FGT-VM64-148_root_health_ip_ts2	> 0 out of 1
<input type="checkbox"/> Import_FGT-VM64-148_root_health_ping2	> 0 out of 1
<input type="checkbox"/> Import_FGT-VM64-148_root_health_ping3	> 0 out of 1
<input type="checkbox"/> Import_FGT-VM64-148_root_health_ping_corp_gw	> 0 out of 1
<input type="checkbox"/> server01	> 0 out of 1
<input type="checkbox"/> server02	> 0 out of 1
<input type="checkbox"/> server03	> 0 out of 1
<input type="checkbox"/> server04	> 0 out of 1
<input type="checkbox"/> port8	> 0 out of 1
<input type="checkbox"/> port9	> 0 out of 1

# Zero Touch Provisioning - CLI Template mit Variablen

- Bei den Meta Felder (Meta Fields) werden die Variablen definiert, welche für die CLI Vorlage verwendet werden.



The screenshot shows the FortiManager System Settings interface. The left sidebar lists various settings categories, with 'Meta Fields' selected at the bottom. The main panel displays a table of Meta Fields. A green box highlights the 'Device' section, which contains the following fields:

Meta Fields	Length	Importance	Status
<strong>System Administrator (2)</strong>			
Contact Email	50	Optional	Enabled
Contact Phone	50	Optional	Enabled
<strong>Device (14)</strong>			
12345678901234567890123456789012	50	Optional	Enabled
12345678901234567890123456789013	20	Required	Enabled
City	50	Optional	Enabled
Company/Organization	50	Optional	Enabled
Contact	50	Optional	Enabled
Country	50	Optional	Enabled
Province/State	50	Optional	Enabled
addr1_2	20	Optional	Enabled
addr1_3	20	Optional	Enabled
addr3	20	Optional	Enabled
device_cli_tmp_test_syntax1_test	20	Optional	Enabled
mask	20	Required	Enabled
vlan112	20	Optional	Enabled
vlan32	20	Optional	Enabled
<strong>Device Group (3)</strong>			
device_group_firmware_test_grp1	20	Optional	Enabled
device_group_firmware_test_grp2	20	Optional	Enabled
device_group_firmware_test_grp3	20	Optional	Enabled
<strong>Administrative Domain</strong>			
<strong>Firewall Address (1)</strong>			



# Zero Touch Provisioning - CLI Template mit Variablen

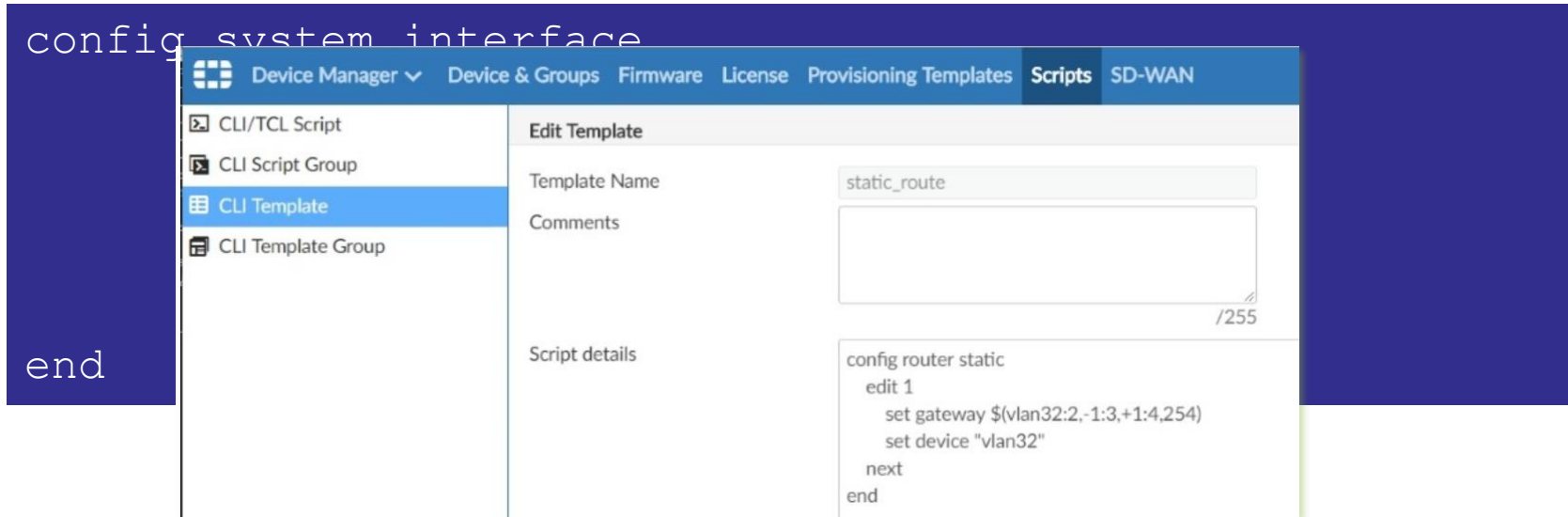
- ▶ Im Device Manager beim entsprechenden Device die gewünschten Werte den Variablen zuweisen.

The screenshot shows the 'Edit Device' form in the FortiManager Device Manager. The device name is FGVMLTM18000204. The form includes fields for Name, Description, IP Address, Serial Number, Firmware Version, Admin User, Password, Connected Interface, HA Mode, Device Location, Geographic Coordinate, Company/Organization, Country, Province/State, City, and a Variables section. The Variables section is highlighted with a green box and contains the following fields:

Variable	Value	Required
addr1_2		Optional
addr1_3		Optional
addr3		Optional
device_cli_tmpl_test_syntax1_test		Optional
mask	255.255.255.0	Required
vlan112		Optional

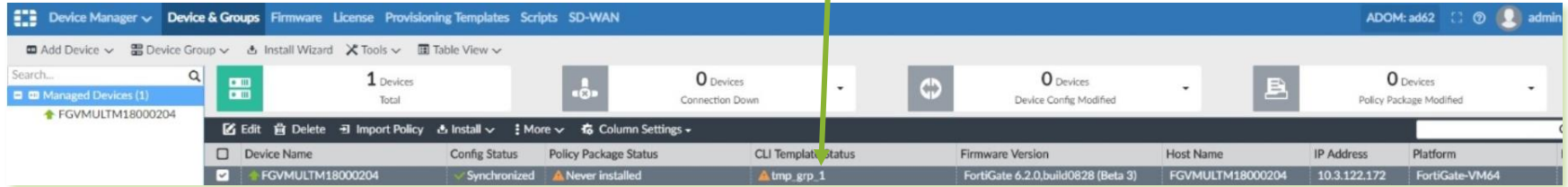
# Zero Touch Provisioning - CLI Template mit Variabeln

► Beispiele eines CLI Templates:



# Zero Touch Provisioning - CLI Template mit Variablen

- Im Geräte Manager kann man die zugewiesenen Templates sehen

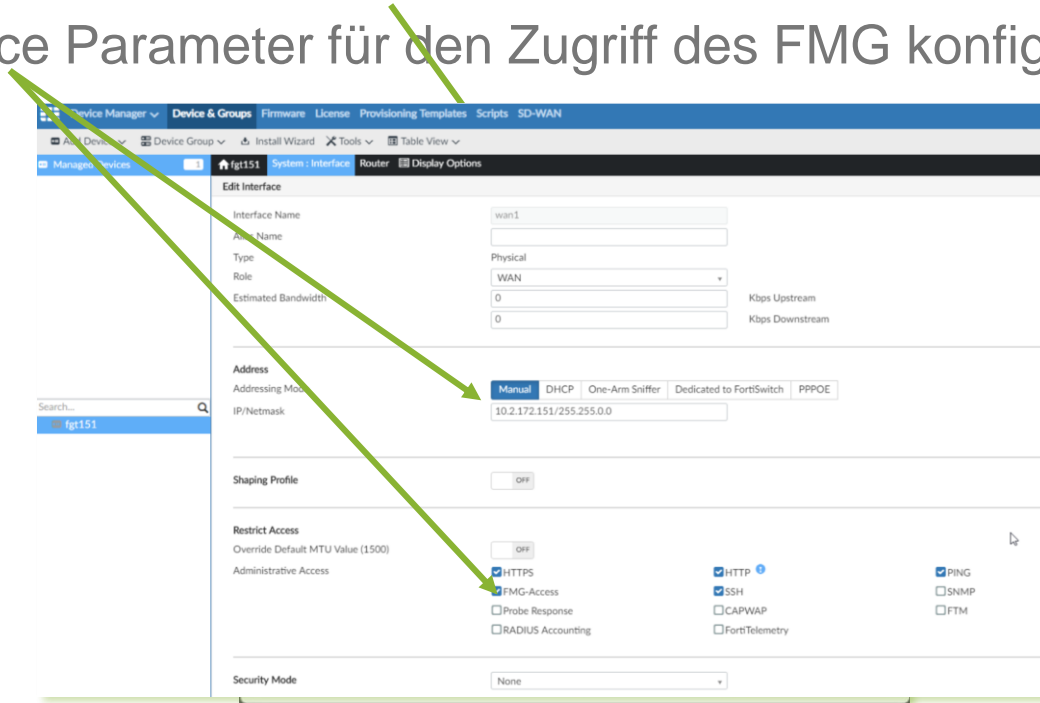


The screenshot shows the FortiManager Device Manager interface. The top navigation bar includes tabs for Device Manager, Device & Groups, Firmware, License, Provisioning Templates, Scripts, and SD-WAN. The main area displays a table of managed devices. A green arrow points from the text 'Im Geräte Manager kann man die zugewiesenen Templates sehen' to the 'CLI Template Status' column of the table.

Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version	Host Name	IP Address	Platform
FGVMULTM18000204	✓ Synchronized	⚠ Never installed	⚠ tmp_grp.1	FortiGate 6.2.0.build0828 (Beta 3)	FGVMULTM18000204	10.3.122.172	FortiGate-VM64

# Zero Touch Provisioning für FortiAP

- ▶ FortiGate mit Seriennummer im FMG erfassen
- ▶ Interface Parameter für den Zugriff des FMG konfigurieren



# Zero Touch Provisioning für FortiAP

- Im AP Manager den AP mit seiner Seriennummer hinzufügen

Add FortiAP

FortiGate: fgt151 (root)

Serial Number: PS311C3U15000439

Name: faps311c-1

AP Profile: FAPS311C-default

OK Cancel

Add FortiAP

100%

Total: 1/1, Success: 1, Error: 0, Warning: 0

Index	Name	Status
1	fgt151	Copy to model device(fgt151) done

Close

AP Manager ▾ Managed APs Monitor Map View WIFI Profiles

FortiAP Group ▾ Install Wizard

Search...

All\_FortiGate (1)

fgt151 (1)

All FortiAPs

1 Managed APs 0 Online 1 Offline 0 Unauthorized

0 Rogue APs

+ Create New Edit Delete Assign Profile More ▾ Column Settings ▾

Access Point	Connected Via	SSIDs	Channel	Clients
<input type="checkbox"/> PS311C3U15000439	--	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0

# Zero Touch Provisioning für FortiAP

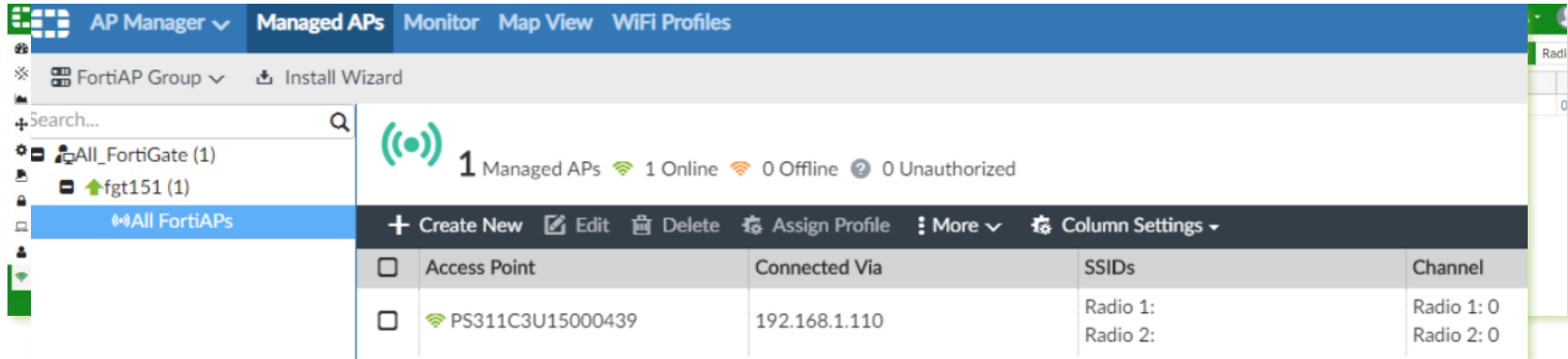
- ▶ AP und FMG Netzwerktechnisch miteinander verbinden
- ▶ Auf der FortiGate den FortiManager konfigurieren.
- ▶ Auf dem FortiManager den Status der Auto-Link Funktion überprüfen

The screenshot displays the FortiGate 80E-POE web interface. The top navigation bar is green with the title 'FortiGate 80E-POE' and a link to 'FortiGate-80E-POE'. Below this, the 'Security Fabric Settings' page is visible, showing 'ADOM: root' and a user 'admin'. The main content area features a 'Central Management' section with a 'Client Connected' status and a 'Push config to device' button. A table lists 'Clients' with columns for 'Radio 1', 'Radio 2', 'OS Version', and 'AP Profile'. The table shows two entries: 'Radio 1: 0' and 'Radio 2: 0'. A 'Status' section at the bottom indicates 'Not Managed'. A yellow warning box on the right states: 'Information from FortiManager and full control of this FortiGate will be lost if you disconnect the FortiGate from 10.2.172.82 at 10.2.172.82'.

Clients	OS Version	AP Profile
Radio 1: 0		
Radio 2: 0		

# Zero Touch Provisioning für FortiAP

- ▶ Auf der FortiGate den Accesspoint überprüfen ob er aktiviert wurde
- ▶ Im FortiManager sollte man den AP jetzt auch online sehen



The screenshot displays the FortiManager 'AP Manager' interface. The top navigation bar includes 'AP Manager', 'Managed APs', 'Monitor', 'Map View', and 'WiFi Profiles'. Below this, a sidebar on the left shows a tree view with 'FortiAP Group', 'All\_FortiGate (1)', 'fgt151 (1)', and 'All FortiAPs' (selected). The main area shows a summary: '1 Managed APs', '1 Online', '0 Offline', and '0 Unauthorized'. Below the summary is a table of managed APs.

Access Point	Connected Via	SSIDs	Channel
<input type="checkbox"/> PS311C3U15000439	192.168.1.110	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0

# Zero Touch Provisioning für FortiSwitch

- ▶ FortiGate auf dem Manager einbinden und Interface für management konfigurieren.
- ▶ FortiLink auf Interface konfigurieren und IP Adresse definieren
- ▶ FortiSwitch mit Seriennummer hinzufügen

The screenshot illustrates the Zero Touch Provisioning (ZTP) process in FortiManager. It shows three overlapping windows:

- Add FortiSwitch (Left):** A form for adding a new FortiSwitch. Fields include:
  - FortiGate: fgt151 (root)
  - Device Interface: dmz
  - Serial Number: S248DF3X17000116
  - Name: fsw248dButtons for OK and Cancel are at the bottom.
- Edit Interface (Middle):** A window for configuring the management interface. It shows fields for Interface Name, Alias Name, Type, Role, and Address. The 'System : Interface' tab is selected.
- Add FortiSwitch (Right):** A confirmation window showing a progress bar at 100%. It displays the total count (1/1), success (1), error (0), and warning (0). A table shows the provisioning status:

Index	Name	Status
1	fgt151	Copy to model device(fgt151) done

A Close button is at the bottom right.

At the bottom, the **Managed Switches** table in FortiManager is visible, showing the newly added switch:

FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version
fsw248d	S248DF3X17000116	FortiSwitch-248D-FPOE	fgt151[root]		



# Zero Touch Provisioning für FortiSwitch

- Ein FortiSwitch Template auf dem FortiManager erstellen und das Template zuweisen

The screenshot displays the FortiManager interface for configuring and assigning FortiSwitch templates. The left sidebar shows the navigation tree with 'FortiSwitch Templates' selected. The main area is divided into two panels: 'Edit FortiSwitch Template' and 'Assign FortiSwitch Template'.

**Edit FortiSwitch Template:**

- Template Name: template-fsw-248d
- Description: Imported from switch S248DF3X17000116
- Platforms: FortiSwitch-248D-FPOE

**Switch VLAN Assignments:**

Port	Native VLAN	Allowed VLAN	Security Policy	LLDP Profile	QoS Policy	POE	DHCP Blocking
port1	vlan101	default.qtnport	FortiSwitch-security-p1	lldp-profile-1	fortswitch-qos-policy-1	Enabled	Untrusted
port2	default.vswport	vlan102		default-auto-isl	default	Enabled	Untrusted
port3	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port4	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port5	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port6	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port7	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port8	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port9	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port10	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port11	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port12	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port13	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
port14	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted

**Assign FortiSwitch Template:**

FortiSwitch Template:

Buttons: OK, Cancel

# Zero Touch Provisioning für FortiSwitch

- Policy Packet für das Model Device erstellen und dies auf das FortiGate Model kopieren.

Install Wizard - Policy Package (fgt151)

✓ Installation Preparation Total: 2/2, Success: 2, Error: 0, Warning: 0

Index	Name	Status
1	Write summary[preview]	Write preview done
2	fgt151[copy] - root	Copy to device done

✓ Interface Validation

✓ Policy and Object Validation

✓ Ready to Install

Device Name	Status	Action
fgt151[root]	Copy Only	Install Preview

Install Cancel

# Zero Touch Provisioning für FortiSwitch

- ▶ FortiGate im Manager einbinden
- ▶ Template zuweisen
- ▶ Konfiguration auf die FortiGate deployen
- ▶ Nach dem pushen der Konfiguration, im FMG den Status refreshen

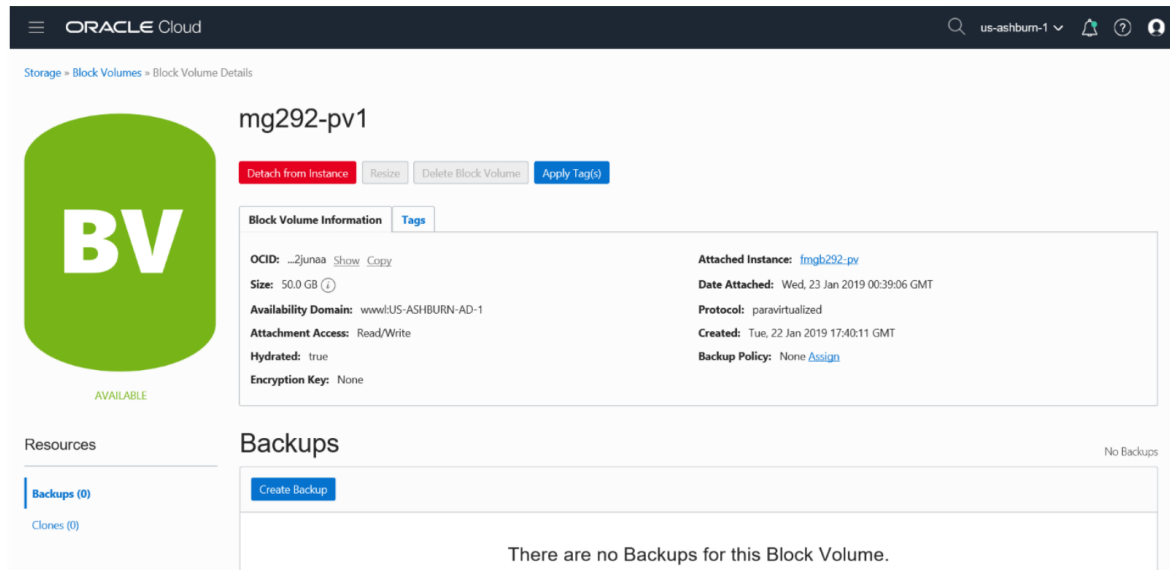
The screenshot shows the FortiSwitch Manager web interface. The top navigation bar includes 'FortiSwitch Manager', 'Managed Switches', 'Monitor', and 'FortiSwitch Templates'. The 'Managed Switches' tab is active. Below the navigation bar, there is a search bar and a summary section showing '1 Managed FortiSwitch' with status indicators for 'Online', 'Offline', and 'Unauthorized'. A table lists the managed switches. The first switch, 'fsw-116', is selected. A context menu is open for this switch, showing options: 'Assign Template', 'Authorize', 'Deauthorize', 'Restart', 'Refresh' (highlighted with a red box), and 'Upgrade'. Below the table, there is a 'Connect to CLI' button.

FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template	Join Time
fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo]	10.10.10.2	S248DF-v3.4-build193	template-fsw-248d	Wed May 15 15:45:59 20

# Multi-Cloud

# Oracle Cloud - Paravirtualized Mode Support

- Der FortiManager unterstützt ab 6.2 den paravirtualisierten Modus in der Oracle Cloud.



# Usability

# Konsolidierter Firewall-Modus

## ► IPv4 und IPv6 Regeln in einem erstellen

The screenshot shows the FortiManager interface for creating a new consolidated policy. The left sidebar shows the tree structure with 'Consolidated IPv4/IPv6 Policy' selected. The main panel is titled 'Create New Consolidated IPv4/IPv6 Policy' and contains the following fields:

- Name: [Empty text box]
- IPv4 Source Address: [all] (with a green box around it)
- IPv6 Source Address: [all] (with a green box around it)
- Source User: [Empty text box]
- Source User Group: [Empty text box]
- IPv4 Destination Address: [all] (with a green box around it)
- IPv6 Destination Address: [all] (with a green box around it)
- Service: [ALL]
- Schedule: [always]
- Action: [Deny] [Accept] [IPSEC]
- Log Traffic: ☒ Log Violation Traffic
- Generate Logs when Session Starts: ☐
- Comments: [Empty text box]
- Advanced Options >

At the bottom right, there are 'OK' and 'Cancel' buttons.

# IPv6 Templates

- Das IPv6-Template ermöglicht es Administratoren, eine IPv6-Vorlage mit vordefinierten Parametern zu erstellen

**Edit IPv6 Address Template**

Name: Addr6Template-offices

IPv6 Address Prefix: 2001:abcd::/96

**Subnet Segments** ⓘ

+ Create New   ✎ Edit Segment   📄 Edit Values for Segment   🗑 Delete

<input type="checkbox"/>	Segment Name	Bits	Exclusive	Defined Values
<input type="checkbox"/>	country	2	Disable	Canada : 0b01 France : 0b10 Germany : 0b11
<input type="checkbox"/>	state	4	Disable	
<input type="checkbox"/>	city	8	Enable	Vancouver : 0b01000001 Burnaby : 0b01000010 Toronto : 0b01000011 Paris : 0b10000001 Berlin : 0b11000001
<input type="checkbox"/>	site	4	Disable	
<input type="checkbox"/>	lan	4	Disable	
<input type="checkbox"/>	vlan	4	Disable	

OK Cancel



# Policy und Routen Lookup

- Policy und Routen können anhand von Eingaben gesucht werden.
- Die Funktionen zur Policy- und Routensuche werden beide über die FortiGate-API aufgerufen, da diese den Echtzeitzustand der FortiGate benötigen.

The top screenshot shows the 'Policy & Objects' section with a search for 'IPv4 Policy lookup from remote device'. The search criteria are: Device/VDOM: FGV08RL00000110 (root), Source Interface: port3, Protocol: TCP, Source: 13.2.119.10, Source Port: Optional (1-65535), Destination: 14.2.119.100, Destination Port: 80. The results table shows three entries:

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		port3	port4	all	all	always	HTTP		Accept
2		port2	port4	all	all	always	AF53		Accept
3	Implicit Deny	any	any	all	all	always	ALL		Deny

The bottom screenshot shows the same search results in a different view, highlighting the 'Implicit Deny' entry.

- ▶ Regeln können in Blöcke definiert werden
- ▶ Die Blöcke können im Regulären Policy Pack hinzugefügt werden.



# Promote Objects LOCAL → GLOBAL

- ▶ Objekte können von einer ADOM in die Globale Datenbank verschoben werden
- ▶ Globale Objekte können für alle ADOMs benutzt werden

The image consists of two screenshots from the FortiManager web interface, illustrating the process of promoting a local object to the global database.

**Top Screenshot:** The interface shows the 'Object Configurations' tab. The top right corner displays 'ADOM: root' and the user 'admin'. A modal window titled 'Rename object(s)' is open, showing a table with columns 'Object Name' and 'New Name'. The table contains one row: 'FIREWALL\_AUTH\_PORTAL\_ADDRESS' in the 'Object Name' column and '2-0' in the 'New Name' column.

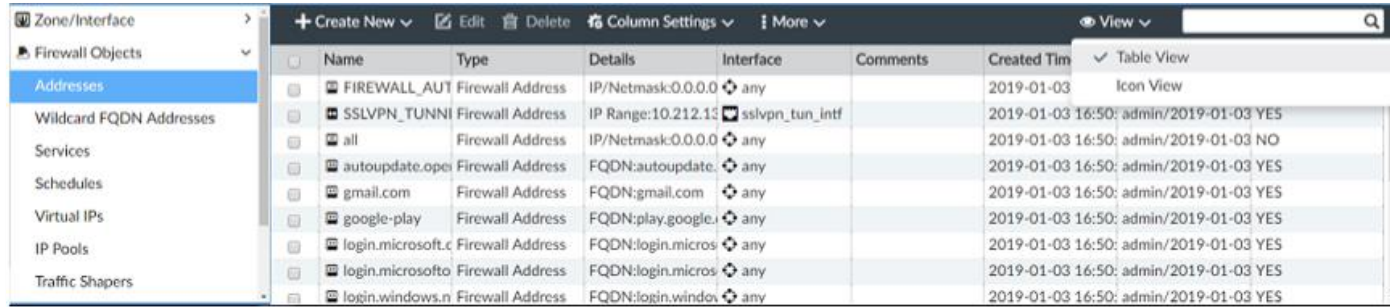
**Bottom Screenshot:** The interface shows the 'Object Configurations' tab. The top right corner displays 'ADOM: Global Database' and the user 'admin'. The left sidebar shows a tree view with 'Addresses' selected. The main table lists objects with columns: Name, Type, Details, Interface, Comments, Created Time, and Last Modified. The table contains the following rows:

Name	Type	Details	Interface	Comments	Created Time	Last Modified
g-10.237.36.181	Firewall Address	IP/Netmask:10.23	any		2019-01-04 12:24	admin/2019-01-0
gFIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
none	Where Used	mask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
swscan.apple.com	Grouping	swscan.ap	any		2018-12-04 11:15	admin/2018-12-0
update.microsoft.com	Promote to Global	update.mic	any		2018-12-04 11:15	admin/2018-12-0

A green box highlights the 'g-10.237.36.181' object in the table. A green arrow points from this object to the 'Promote to Global' button in the bottom row of the table.

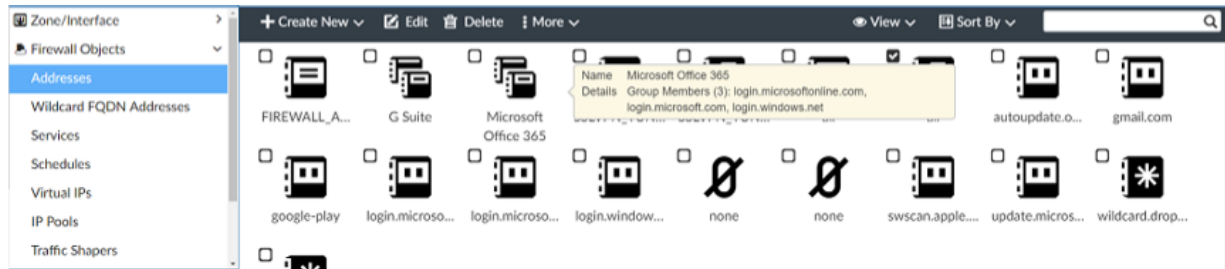
# Adresssymbol / Kachelansicht

## ► Adresssymbol Ansicht:



Name	Type	Details	Interface	Comments	Created Time
FIREWALL_AUT	Firewall Address	IP/Netmask:0.0.0.0	any		2019-01-03
SSLVPN_TUNNI	Firewall Address	IP Range:10.212.11	sslvpn_tun_intf		2019-01-03 16:50: admin/2019-01-03 YES
all	Firewall Address	IP/Netmask:0.0.0.0	any		2019-01-03 16:50: admin/2019-01-03 NO
autoupdate.open	Firewall Address	FQDN:autoupdate.open	any		2019-01-03 16:50: admin/2019-01-03 YES
gmail.com	Firewall Address	FQDN:gmail.com	any		2019-01-03 16:50: admin/2019-01-03 YES
google-play	Firewall Address	FQDN:play.google.com	any		2019-01-03 16:50: admin/2019-01-03 YES
login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		2019-01-03 16:50: admin/2019-01-03 YES
login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		2019-01-03 16:50: admin/2019-01-03 YES
login.windows.net	Firewall Address	FQDN:login.windows.net	any		2019-01-03 16:50: admin/2019-01-03 YES

## ► Kachel Ansicht



# Device Manager Map View

- ▶ Grün = OK, Koordinaten der FortiGate angeben
- ▶ Gelb = Warnung → Synchronisation nicht I.O FortiGate und FMG
- ▶ Rot = Fehler → Installation Fehlgeschlagen, Gerät nicht erreichbar.

Device Manager | Device & Groups | Firmware | License | Provisioning Templates | Scripts | SD-WAN | ADOM: adom60 | admin

Map View

Device Name	Geographic Coordinate	City	Country
FGVM02AO20311101	49.2488091, -122.9805104	Burnaby	Canada
FGVM02AO20311102	0, 0	Unknown Location	Democratic Republic of the Congo
vlan111_001	38.5481654230466, -80.33203125	Webster Springs	United States
vlan111_002	45.089035564831, 0.87890625	Saint-Pierre-de-Chignac	France
vlan111_003	0, 0	Alexandria	United States
vlan111_004	37.36883, -122.0363496	Sunnyvale	United States
vlan111_005	38.0513317765517, -119.33546875	Tipton	United States
vlan111_006	0, 0	Sunnyvale	United States
vlan111_007	50.9584267233599, 8.61328125	Battenberg (Eder)	Germany
vlan111_008	36.2088230928372, -115.0048828125	Las Vegas	United States
vlan111_011	52.7259844176303, -108.9613773	Cut Knife	Canada
vlan111_013	43.6158017, 7.05424770000002	Valbonne	France
vlan111_014	40.7511838, -73.9921394	New York	United States
vlan111_015	40.7511838, -73.9921394	New York	United States
vlan111_016	33.8704155509418, -100.8984375	Roaring Springs	United States
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_019	47.6062095, -122.3320708	Seattle	United States
vlan111_020	0, 0	Unknown Location	Unknown Location

Map View: Sunnyvale, CA, USA

Drag to Desired Location

# Klonen von Reversen Policies

- Policy gegengleich konfigurieren (Source und Destination umdrehen)

The screenshot shows the FortiManager interface with a policy package named 'FGVM01SYNTAX0013'. A context menu is open over a policy block, showing options like 'Insert Above', 'Insert Below', 'Clone', and 'Clone Reverse'. The 'Clone Reverse' option is highlighted with a green box. A green arrow points from this option to the 'Destination' column of the cloned policy block in the table below.

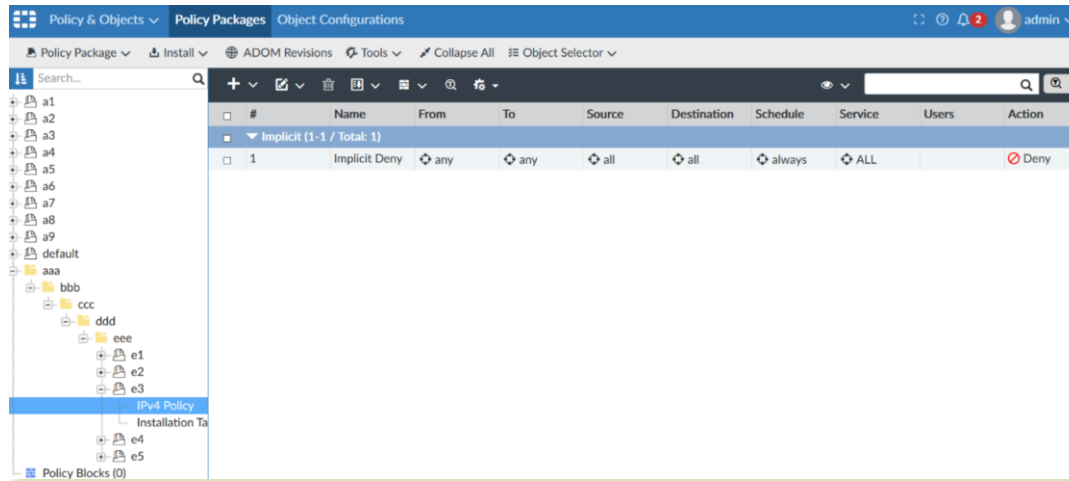
#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile: Log	NAT	Comments	Install On
1		port1	port2	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
2		port2	port1	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
3		port6	port6	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
4		any	any	all	all	always	ALL		Deny	No Log			Install

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile: Log	NAT	Comments	Install On
1		part1	part2	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
2		part2	part1	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
3		part3	part4	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
4		part5	part6	all	all	always	ALL		Accept	Log All Sessions	Disabled		Install
Implicit (5-5 / Total: 1)													
5	Implicit Deny	any	any	all	all	always	ALL		Deny	No Log			Install

# Admin Preference - Policy Package Cookie

- ▶ Zuletzt geöffnetes Policy Package wird beim erneuten einloggen geöffnet.
- ▶ Das zuletzt bearbeitete Objekt wird beim erneuten einloggen wieder geöffnet





# Upgraden von Devices

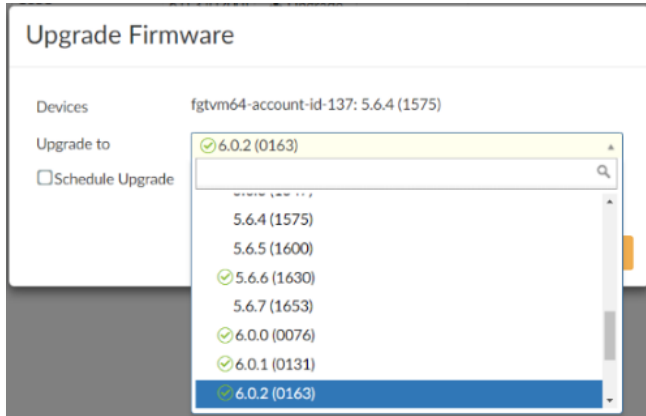
- Warnung beim Upgrade auf eine höhere Version von FortiOS als FortiManage





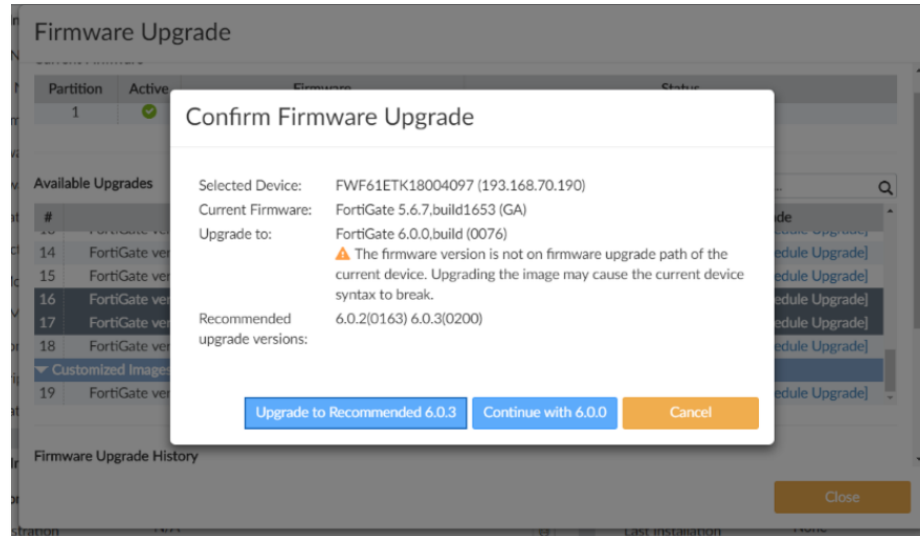
# Upgraden von Devices

- Aktualisieren mehrerer FortiGate Devices mit dem empfohlenen Upgrade Pfad



# Individuelles Aktualisieren mit empfohlenem Upgrade Pfad

- Wenn eine Firmware ausgewählt wird die sich nicht auf dem upgrade Pfad befindet, wird eine Warnung mit der Option zum Aktualisieren mit dem empfohlenen Upgrade Pfad angezeigt.



# Spanische Oberfläche

**View Settings**

Language: English  
Theme: [Search]

Auto Detect  
English  
Simplified Chinese  
Traditional Chinese  
Japanese  
Korean  
Spanish

**Ajustes de Sistema**

Tablero  
Registrando Topología  
Todos los ADOMs  
Información de almacenamiento  
Administrador RAID  
Red  
HA  
Admin  
Administrador  
Perfil  
Servidor Remoto de Autenticación  
Configuración de Administración  
Certificados  
Certificados Locales  
Certificados CA  
CRL  
Reenvío de registros  
Administración de búsqueda  
Log de Eventos  
Monitor de Tareas  
Avanzado  
SNMP  
Servidor de Correo  
Servidor Syslog  
Meta Campos  
Ajustes del registro de Dispositivo  
Administración de Archivos  
Ajustes Avanzados

**Información del Sistema**

Nombre del Host: FAZ300F  
Número Serial: FL-3HF3917900018  
Hora del Sistema: Fri Feb 22 14:51:12 2019 PST  
Versión de Firmware: v6.2.0-build1005 190215 (Interim)  
Configuración del Sistema: Último Respaldo: N/A  
Administradores: admin / 2 en total  
Actuales  
Tiempo de Actividad: 3 días 2 horas 55 minutos 54 segundos  
Dominio Administrativo: ON  
Modo de Operación: Analizador Colector

**Recursos del Sistema**

Uso promedio de CPU (Detalles del Multi-Core): 7%  
Uso de Memoria: 19%  
Uso de Disco: 1%

**Información de la Licencia**

Registro: Dispositivos/VDOM: 46 of 180  
GB/Day: 0.0 of 150 (0.0%)  
FortiGuard: Servicio de Indicadores de Compromiso: Sin Licencia  
Ubicación del Servidor: Servidores Ubicados en US solamente  
Actualizar servidor: AntiVirus e IPS: 96.45.33.87 Sunnyvale, California, United States  
Actualización del FortiClient: 96.45.33.105 Sunnyvale, California, United States

**Unidad de Operación**

**FORTINET**  
FortiAnalyzer-300F  
Reiniciar Apagado

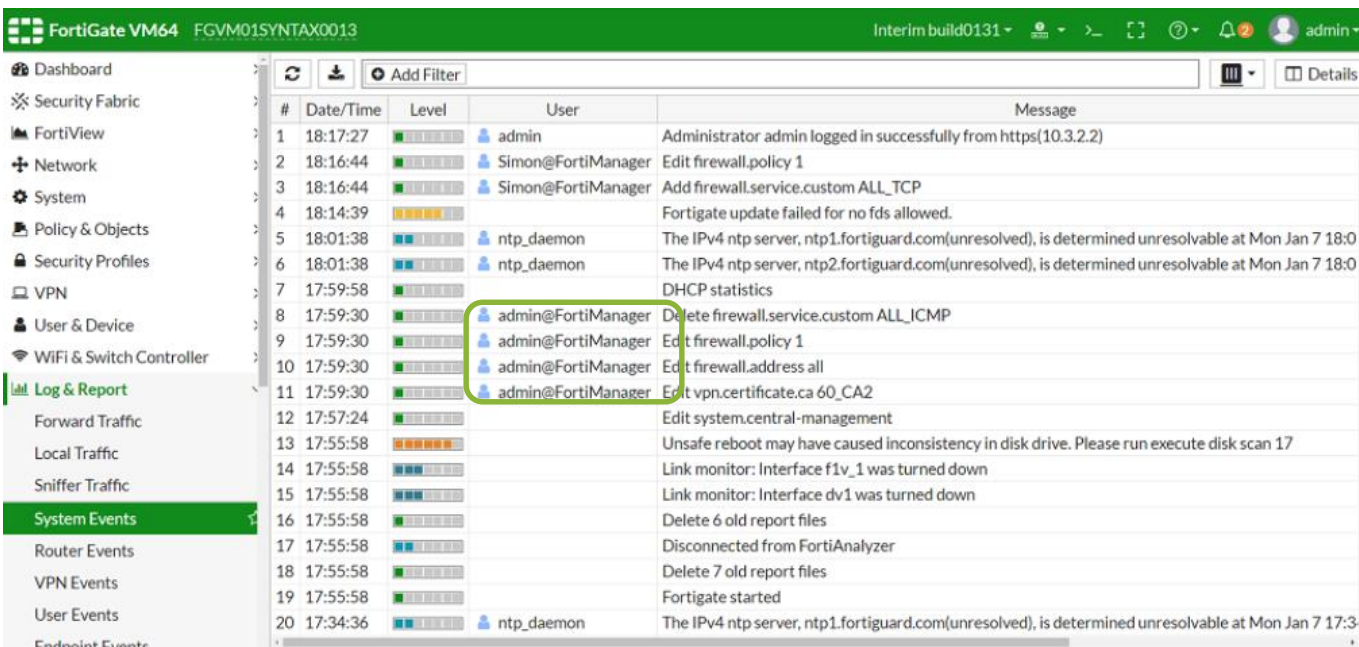
**Consola de Mensajes de Alerta**

Tiempo	Mensaje
Feb 22, 14:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 13:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 12:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 11:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22,	The created ADOM number is 26, which exceeded the recommended

# Compliance

# Änderung Change Log auf der FortiGate

- Wenn eine Änderung auf der FortiGate durch den FortiManager vorgenommen wird, ist diese jetzt klarer im Change Log ersichtlich



FortiGate VM64 FGV01SYNTAX0013 Interim build0131 admin

Dashboard  
Security Fabric  
FortiView  
Network  
System  
Policy & Objects  
Security Profiles  
VPN  
User & Device  
WiFi & Switch Controller  
**Log & Report**  
Forward Traffic  
Local Traffic  
Sniffer Traffic  
**System Events**  
Router Events  
VPN Events  
User Events  
Endpoint Events

#	Date/Time	Level	User	Message
1	18:17:27		admin	Administrator admin logged in successfully from https(10.3.2.2)
2	18:16:44		Simon@FortiManager	Edit firewall.policy 1
3	18:16:44		Simon@FortiManager	Add firewall.service.custom ALL_TCP
4	18:14:39			Fortigate update failed for no fds allowed.
5	18:01:38		ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 18:0
6	18:01:38		ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 18:0
7	17:59:58			DHCP statistics
8	17:59:30		admin@FortiManager	Delete firewall.service.custom ALL_ICMP
9	17:59:30		admin@FortiManager	Edit firewall.policy 1
10	17:59:30		admin@FortiManager	Edit firewall.address all
11	17:59:30		admin@FortiManager	Edit vpn.certificate.ca 60_CA2
12	17:57:24			Edit system.central-management
13	17:55:58			Unsafe reboot may have caused inconsistency in disk drive. Please run execute disk scan 17
14	17:55:58			Link monitor: Interface f1v_1 was turned down
15	17:55:58			Link monitor: Interface dv1 was turned down
16	17:55:58			Delete 6 old report files
17	17:55:58			Disconnected from FortiAnalyzer
18	17:55:58			Delete 7 old report files
19	17:55:58			Fortigate started
20	17:34:36		ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 17:3

# Modifikation Event Log

- ▶ Die Session ID wird zu jedem Logeintrag hinzugefügt
- ▶ Vorhandene Prüfsumme Linux Epochen-Zeitstempel, wird ein ein für Menschen Lesbares Format konvertiert
- ▶ ADOM Preempt Lock Takeover Event Logs sind klarer.

The screenshot displays the FortiManager web interface. The top navigation bar includes 'System Settings' and user information 'ADOM: root' with an 'Unlock' button. The left sidebar shows a menu with 'Event Log' selected. The main content area shows a table of events with columns for 'Description' and 'Message'. The events are filtered for the last day, from February 21 to February 22. The table lists several events related to user login/logout and session management for 'ADMIN2' and 'ADMIN1'.

	Description	Message
nager event	Session manager event log	The session 53095 of the user 'ADMIN2' from jsconsole(192.168.1.110) is killed
nager event	User login/logout successful	user 'ADMIN2' with profile 'Super_User' login accepted from jsconsole(192.168.1.110)
nager event	Adom locked/unlocked/switched	The previous lock was removed from ADMIN1 (51909). User 'ADMIN2' locked adom (root) from 'GUI(192.168.1.110)'
nager event	Adom locked/unlocked/switched	User 'ADMIN2' (from 'GUI(192.168.1.110)') lock adom (root) success
nager event	Adom locked/unlocked/switched	User 'ADMIN1' (from 'GUI(192.168.1.110)') unlock adom (root) success
nager event	Adom locked/unlocked/switched	User 'ADMIN1' (from 'GUI(192.168.1.110)') lock adom (root) success
nager event	User login/logout successful	User 'ADMIN2' with profile 'Super_User' login accepted from GUI(192.168.1.110).
nager event	User login/logout successful	User 'ADMIN1' with profile 'Super_User' login accepted from GUI(192.168.1.110).
nager event	User login/logout successful	User 'admin' with profile 'Super_User' login accepted from GUI(192.168.1.110).

# Other

# Löschen von leeren ADOMs

- ▶ Alle Devices müssen in einer ADOM entfernt werden
- ▶ Die globalen Verknüpfungen werden neu gelöscht, wenn die ADOM gelöscht wird

### ADOM Reference(s) Detected

ADOM 'test-ADOM' is being referenced by the following object(s).

#	Object Name	Object Key
1	system admin user (System Settings)	test-admin
2	policy (Global Database)	default

Force to delete these ADOM(s) would result in reference clean up.

Delete AnywayCancel



# Modifiziertes RADIUS Setting

- ▶ Testen der User Credentials
- ▶ Die Wildcard-Option wurde geändert, um alle Benutzer auf dem Remote-Server in der GUI abzugleichen.

```
config system admin user
  edit "Radius"
    set adom "all_adoms"
    set policy-package "all_policy_packages"
    set user_type radius
    set radius_server "test-Radius"
    set wildcard enable
    set ext-auth-accprofile-override enable
    set ext-auth-adom-override enable
  next
end
```